OSX USE OF CLOUD STORAGE APPLICATIONS FOR INTELLECTUAL PROPERTY THEFT
(Revised December 2018)

Anthony Martinez[12]

[1]Viterbi School of Engineering, Information Technology Program, University of Southern California, Los Angeles, CA 90007, USA
[2]Viterbi School of Engineering, Department of Computer Science, University of Southern California, Los Angeles, CA 90007, USA

Intellectual property theft cases are among some of the most common cases that cyber security professionals experience. They account for roughly 31 percent of all cyber security related incidents [1]. Amongst these cases, there are often instances of attackers accessing information from a company's cloud infrastructure. There are two main cloud components: Dropbox and iCloud. Both cloud environments can share files, with iCloud having the ability to share apple related features such as calendar events or email. The persistent syncing of all documents makes both tools incredibly powerful, yet dangerous of access were to fall in the wrong hands.

***Index Terms*—exfiltration, cloud, Dropbox, iCloud, forensics**

I. Introduction

Dropbox and iCloud are two common cloud infrastructures that are used for the sharing and distribution of material across various computers and networks. This report details some of the forensic artifacts left behind simply on syncing the cloud application account on a fresh device.

II. Procedures

A. Environment setup

The researcher set up the proper environment to conduct the research, using a clean partition to establish a baseline. The examiners created six total partitions. On three of the partitions they installed MAC OS X High Sierra version 10.13.5. On the other three partitions, they installed MAC OS X Mojave version 10.14.1. The researcher conducted all forensic research on these six systems. All six partitions were split into three groups each with one 10.13.5 system and 10.14.1 system. One group was for a clean install. This would be our control group to compare all findings to. The second group would be for Dropbox. All Dropbox related research would occur here. The third group would be for iCloud. All iCloud related research would be conducted here.

In addition to these six systems, the researcher used one additional system. This system, located on the same hard drive but in a different portion, was to create an online Dropbox account, establish and create an iCloud account, and convert all six portions into forensic images.

There are various account names that were used to create accounts. The paper may refer to them. For reference:

- Gmail: itp445project@gmail.com
- iCloud: itp445project@icloud.com

B. Dropbox Setup

As previously mentioned, all Dropbox setup was conducted on a separate machine from the six partitions that the forensic research was conducted on. The following procedure details the various steps used to create the test data for Dropbox:

1. Dropbox account creation: The researcher created an account on “dropbox.com” using the test Gmail address and unique password.
2. Following the creation of the account, the researcher created five files on a separate device: a .zip, .pdf, .txt, .docx, and .jpg. These were chosen due to them being most commonly present in a business setting.
3. The researcher used the separate device to log into the Dropbox test account and manually upload the test files.
4. Upon successful upload, the researcher started the test device and downloaded the Dropbox.dmg installation file. The researcher then installed Dropbox with the default parameters[3].
5. The researcher then allowed for Dropbox to run and sync files. The test device was powered off immediately after and imaged.[4]

C. iCloud Setup

As previously mentioned, all iCloud setup was conducted on a separate machine from the four that forensic research is being conducted on. The following procedure follows the various

[3] Default non-business account
[4] Imaging was done on the external system with live imaging using dd, specific command can be found in the appendix

steps that the research took to add data into iCloud.

1. iCloud creation. The researcher obtained access to a Mac computer. Using this Mac computer, they created an iCloud account. For actual account setup steps please visit https://support.apple.com/en-us/HT208682.
2. Following the creation of the account the researcher added the same test files used for the Dropbox setup.
3. iCloud Drive: The researcher added the test files into iCloud drive
4. iPhoto: The researcher added a single photo into iPhoto. It is important to note that they turned on iCloud photo sharing. This setting enables the Photos application to sync the data to iCloud
5. iCalendar: the researcher added two events to iCalendar. One event was created under itp445project@gmail.com. The other two events that were created were under itp445project@icloud.com.
6. Email: The researcher sent an email from itp445project@icloud.com to itp445project@gmail.com
7. Notes: The researcher created a note on iCloud
8. Contacts: The researcher added two contacts with varying information, such as their birthdays.
9. Following the creation of all the iCloud elements, the researched allowed iCloud to sync.

The researcher added all the previous elements for two reasons. The first was because of their importance in a business intellectual property case. These locations were all areas that the researcher identified that might have critical or sensitive business information stored. The second reason was that the researcher wanted to determine that if how much of the data would actual sync over, especially if attackers were able to obtain unauthorized access.

Following the completion of the iCloud creation and file syncing, the researcher booted up both iCloud test environments. Following startup, each of the systems was logged into iCloud. After allowing for sufficient time for all files to sync the researcher shut down the system.

D. *Image Creation*

To get an image of the two iCloud partitions, the researcher logged into a third system, located on a different partition on the same hard drive. After logging in the researcher ran a command that would create a dd file of the entire partition as well as an Md5.txt file [2]. The command can be found in the appendix**.**

E. Analysis

Following the creation of the dd images, the researcher loaded the dd image files into Blacklight for analysis and allowed the processing to complete.

III. Dropbox

The researcher determined that there were no significant evidentiary differences between the Dropbox application on High Sierra and Mojave. They both left the same artifacts, with Mojave leaving more logging data, as detailed later.

Installation:

Aside from actual content folders created, the researcher identified two files that contained information on the installation of Dropbox: install.log (private/var/log/install.log) and system.log (private/var/log/system.log). The installation log contained 1070 instances of Dropbox (in the Mojave version) compared to just 144 instances [5]in the clean install.

.Dropbox folder:

Researcher located a hidden folder called "~/.dropbox" located in the root of the user's directory. According to Dropbox, Inc., this folder keeps track of information about the users main Dropbox folder as well as shared folders [2]. This folder contained various files, however of most note were those located in "~/.dropbox/instance1" and "~/.dropbox/instance_db".

The "~/.dropbox/instance1" contained various ".dbx" files. These DBX files are encrypted using the SQLite Encryption Extension [3] [4]. They have not been thoroughly studied on OSX systems, with many current tools only able to parse these files for Windows devices [5]. The Windows equivalent description of these files indicates that they are configuration and log files use by Dropbox.

- One of the files for example is the "filecache.dbx" which contains an SQLite record of the names of files in the Dropbox folder, their local filename, their local size, as well as their local creation and modified time. [5]
- Not every one of the ten ".dbx" files located was encrypted. For example, the "aggregation.dbx" file was not encrypted, recognized as a SQLite file, and contained information such as the names of the test files and their timestamp in Unix format (See Appendix for some of the contents of the aggregation file)
- Both the "~/.dropbox/instance_db" and the "~/.dropbox/instance1" folders contained a file called "hostkeys". The files contain two separate, 81-byte strings. These files can be used to decrypt the ".dbx" files into ".db" files. [4] See the Future Work section for more.

The researcher also located the main Dropbox folder, also located in the root of the user's directory (~/Dropbox). The

[5] The instances in the clean install can be explained by OSX having some native support for dropbox.

"~/Dropbox" folder contains the user's uploaded files as well as a cache. The ".dropbox.cache" is a hidden folder stored in the root of the Dropbox folder which contains a cache of files for staging, downloading, uploading, and files that were deleted. [6] The folder is automatically cleared every three days, however can also be manually deleted. It is of significant evidentiary value to search this location as well in the event there's suspicion of deleted files.

Plists

The researcher found 23 Plists whose file name or file path contained Dropbox (see Appendix for complete list). They did not contain anything of significant evidentiary value; as stated above, Dropbox mainly uses the encrypted '.dbx' files to store its configuration and log data**.** It is important to note that none of the 23 Plists were found on the clean install. This indicated that all 23 Plists were created from the Dropbox install.

IV. Dropbox High Sierra vs Dropbox Mojave

The researcher compared the results of High Sierra to the results from Mojave. One of the first noticeable comparisons was the overall number of Dropbox files. In High Sierra, there were a total number of 803 total files that we identified were associated to Dropbox or the contents placed within Dropbox. Mojave had a total number of 631 total files.

The primary storage and database records for both HS and Mojave were still the exact same. Additionally, all 23 plists that were identified to be created by Dropbox were found in the same location.
Ultimately, the two different operating systems appeared to have very little difference to the main core files that Dropbox utilized.

V. iCloud

The researcher determined the following about various iCloud items:

Mail

The researcher located the iCloud emails, indicating they were synced to the device. They were found in the "~/Library/Mail/" directory, along with their attachments.

iCloud Drive

The researcher located the files which were placed in the iCloud drive, indicating that they were also synced to the device. They were in "~/Library/Mobile Documents/com~apple~CloudDocs".

Calendar

The researcher determined that the iCloud, but not the Google, calendar events were synced for both High Sierra and Mojave. Mojave did not sync the calendar birthdays for the contacts on the device, while High Sierra did. The location of the associated artifact is "~/Library/Calendars".

Contacts

The researcher determined that the contacts were synced. The artifact location is "~/Library/Application Support/AddressBook/Sources".

Notes

The researcher determined that notes were not synced to the device.

VI. iCloud: High Sierra vs Mojave

Both systems were practically identical. However, there was one minor difference: contacts syncing. To preface, both contacts that were created had birthdays inputted in the contact information. In High Sierra, the

Issues and Future Research

The researcher identified two main areas that they could expand upon their research: the encrypted .dbx files and the effects of deleting items from both Dropbox and iCloud.

1) Parsing Encrypted DBX Files

The researcher determined that Dropbox uses encrypted SQLite database files for storing various configuration and logging data. These files were found to be stored in the "~/.dropbox" hidden folder. While not all the DBX files stored there were encrypted, the ones which have shown evidentiary evidence in the past are. Specifically, the "filecache", "config", and "deleted" .dbx files. In Windows research of this topic, those files were found to contain information such as names of deleted files, creation times of files, and evidence of files located on the cloud but not synced to the device.

The researcher determined from examining the SQLite Encryption Extension (SEE) documentation that the "hostkeys" files located in the "~/.dropbox/instance1" and "~/.dropbox/instance_db" are a factor in the DBX decryption. Future work would revolve around studying the specific implementation of the SEE encryption and writing a program to take advantage of the key files to decrypt the DBX files for inspection. Currently, this work has not been reported done on an OSX device, so this will be the next project for the researcher.

2) Results of Deleting Data From Dropbox and iCloud

In a real-world scenario, data that is exfiltrated from cloud accounts will not always remain. Sometimes, attackers, once they have exfiltrated data, will attempt to delete data in an attempt to cover their tracks. One of the future areas of research might focus on the effects of deleting data. For both Dropbox and iCloud, the researcher would attempt to delete all the files that were intentionally created or placed. The researcher would then analyze the remaining images for any artifacts that remain of either Dropbox or the information stored within Dropbox.

VII. Conclusion

The goal was to discover what information was available as a result of as single syncing of two common cloud applications, Results were conducted on two different versions of operating system, Mac OS X High Sierra and Mac OS X Mojave to determine what, if any, differences would occur. The researcher was able to determine the main file directories that Dropbox stores all its data in. Additionally, all iCloud related material loaded into iCloud was found and discovered. The comparisons between the two operating system versions revealed that both OSs had all the main file locations stored in the exact same locations.

VIII. Appendix

Figure 1 Plists with "Dropbox" in file name or file path

Path
/Users/cleaninstallhs/Library/Preferences/com.dropbox.tungsten.helper.plist
/Users/cleaninstallhs/Library/Preferences/com.getdropbox.dropbox.plist
/Users/cleaninstallhs/Library/Preferences/com.dropbox.DropboxMacUpdate.plist
/Users/cleaninstallhs/Library/Dropbox/DropboxMacUpdate.app/Contents/Frameworks/CrashReporter.framework/Versions/A/Resources/Info.plist
/Users/cleaninstallhs/Library/Dropbox/DropboxMacUpdate.app/Contents/Info.plist
/Users/cleaninstallhs/Library/LaunchAgents/com.dropbox.DropboxMacUpdate.agent.plist
/Users/cleaninstallhs/Library/Containers/com.dropbox.foldertagger/Container.plist
/Users/cleaninstallhs/Library/Containers/com.dropbox.foldertagger/Data/Library/Preferences/com.apple.security.plist
/Users/cleaninstallhs/Library/Containers/com.dropbox.foldertagger/Data/Library/Preferences/com.apple.security_common.plist
/Users/cleaninstallhs/Library/Containers/com.getdropbox.dropbox.garcon/Container.plist
/Users/cleaninstallhs/Library/Containers/com.getdropbox.dropbox.garcon/Data/Library/Preferences/com.apple.security.plist
/Users/cleaninstallhs/Library/Containers/com.getdropbox.dropbox.garcon/Data/Library/Preferences/com.apple.security_common.plist
/Applications/Dropbox.app/Contents/PlugIns/garcon.appex/Contents/Info.plist
/Applications/Dropbox.app/Contents/Resources/DropboxQL.qlgenerator/Contents/Info.plist
/Applications/Dropbox.app/Contents/Resources/DropboxMacUpdate.app/Contents/Frameworks/CrashReporter.framework/Versions/A/Resources/Info.plist
/Applications/Dropbox.app/Contents/Resources/DropboxMacUpdate.app/Contents/Info.plist
/Applications/Dropbox.app/Contents/XPCServices/DropboxFolderTagger.xpc/Contents/Info.plist
/Applications/Dropbox.app/Contents/XPCServices/DropboxActivityProvider.xpc/Contents/Info.plist
/Applications/Dropbox.app/Contents/XPCServices/DropboxNotificationService.xpc/Contents/Info.plist
/Applications/Dropbox.app/Contents/Frameworks/Tungsten.framework/Versions/A/Resources/Info.plist
/Applications/Dropbox.app/Contents/Frameworks/Tungsten.framework/Versions/A/Frameworks/Dropbox Web Helper.app/Contents/Info.plist
/Applications/Dropbox.app/Contents/Frameworks/Tungsten.framework/Versions/A/Frameworks/Chromium Embedded Framework.framework/Resources/Info.plist
/Applications/Dropbox.app/Contents/Info.plist

Figure 2 Some Contents from "~/.dropbox/instance1/aggregation.dbx"

Timestamp	Server Path
1543876190	4477400928:/README.txt
1543876187	4477400928:/greenfield_l.jpg
1543876188	4477400928:/Money.docx
1543876189	4477400928:/Money.pdf
1543876190	4477400928:/Money.zip

Figure 3 Template of command used on Mac Terminal to create a dd image of the partition

<table>
<tr><th>Terminal Command for dd.</th></tr>
<tr><td>dd if=/dev/rdisk1 bs=4k conv=sync,noerror | tee /Volumes/MAC-Images/my-image.dd | md5 > /Volumes/MAC-Images/my-image-md5.txt</td></tr>
</table>

IX. References

[1] Kroll, "Global Fraud & Risk Report," 2018.

[2] Dropbox, ""Dropbox" folder on Windows and Mac computers," [Online]. Available: https://www.dropbox.com/help/desktop-web/hidden-folder. [Accessed 3 December 2018].

[3] F. Picasso, "Brush up on Dropbox DBX Decryption," Zena Forensics, 30 April 2017. [Online]. Available: http://blog.digital-forensics.it/2017/04/brush-up-on-dropbox-dbx-decryption.html. [Accessed 3 December 2018].

[4] N. Ruff and F. Ledoux, "A Critical Alanysis of Dropbox Software Security," 2012. [Online]. Available: http://archive.hack.lu/2012/Dropbox%20security.pdf. [Accessed 3 December 2018].

[5] Magnet Forensics, "Decrypting the Dropbox filecache.dbx file," 1 March 2013. [Online]. Available:

https://www.magnetforensics.com/computer-forensics/decrypting-the-dropbox-filecache-dbx-file-new-free-tool/. [Accessed 3 December 2018].

[6] Dropbox, "How to clear the cache folder," [Online]. Available: https://www.dropbox.com/help/desktop-web/cache-folder. [Accessed 3 December 2018].

[7] az4n6, "Another Forensics Blog," 6 July 2016. [Online]. Available: http://az4n6.blogspot.com/2016/07/how-to-image-mac-using-single-user-mode.html. [Accessed 03 December 2018].

[8] F. McClain, "Digital Forensics: Dropbox," SANS DFIR, 17 June 2011. [Online]. Available: https://digital-forensics.sans.org/blog/2011/06/17/digital-forensics-rain-drop-keeps-falling-on-my-box. [Accessed 3 December 2018].